Permyakova Elizaveta Andreevna
Student
Ural Federal University
Russia, Ekaterinburg
Academic supervisor: Kovaleva Alexandra Georgievna

THE USE OF COMPUTER FORENSICS METHODS IN THE INVESTIGATION OF MONEY LAUNDERING CRIMES

Abstract. *Financial offenses are a threat to the economic security of any country. Computer forensics are of particular importance in the fight against crime in the studied industry. Computer forensics participates in the implementation of tasks by providing the means and methods to law enforcement agencies and private security services involved in the detection, prevention and investigation of cybercrimes. Thus, the paper considers both fraudulent schemes money laundering and countering them.*

Keywords: *Ural Federal University (UrFU), information security, money laundering, FATF, cyberattack, computer forensics, phishing.*

Пермякова Елизавета Андреевна
Студент
Уральский федеральный университет имени первого
Президента России Б.Н. Ельцина
Россия, г. Екатеринбург
Научный руководитель: Ковалева Александра Георгиевна

ПРИМЕНЕНИЕ МЕТОДОВ КОМПЬЮТЕРНОЙ КРИМИНАЛИСТИКИ ПРИ РАССЛЕДОВАНИИ ФИНАНСОВЫХ ПРЕСТУПЛЕНИЙ, СВЯЗАННЫХ С ОТМЫВАНИЕМ ДЕНЕЖНЫХ СРЕДСТВ

Аннотация. *Правонарушения в финансовом секторе представляют угрозу экономической безопасности любой страны. Особое значение в деле борьбы с преступностью в исследуемой отрасли отводится компьютерной криминалистике, которая участвует в реализации задач путем предоставления своих средств и методов правоохранительным органам и частным службам безопасности, участвующим в выявлении, предупреждении и расследовании киберпреступлений. Так, в статье рассматривается как мошеннические схемы по отмыванию денежных средств, так и противодействие им.*

Ключевые слова: *Уральский Федеральный Университет (УрФУ), информационная безопасность, отмывание денежных средств, ФАТФ, кибератака, компьютерная криминалистика, фишинг.*

Today the proliferation of banking Trojans and regular targeted attacks by hackers on the financial sector are generating opportunities for multimillion dollar profits. The successful solution of the problems of optimizing the practice of combating crime in the financial sector is carried out due to computer forensics, which participates in the implementation of tasks, providing its tools and methods to law enforcement agencies and private security services involved in the investigation of financial crimes 0,0.

The purpose of the study is to analyse common issues related to regulation of and fight with cybercrime in the financial sector and a comparative analysis of the best practices of the implementation of digital technologies to counter cyberattacks around the world.

Appropriate measures have been created to prevent the growing threats in response to the evolution of financial crimes. In 1989, the foundation of the financial action task force was created to counter money laundering. The main task of this organization is to study methods of money laundering, analyze actions taken at the national or international level, and also enable developed countries to strengthen their control over the world monetary and financial system and the rule of law in it. Thus,

the FATF's responsibilities include combating the financing of terrorism, ways to counter the proliferation of weapons of mass destruction, as well as creating tools for a more decisive fight against corruption. The FATF currently consists of 39 jurisdictions and two regional organizations and more than 20 bodies have observer status 0.

The statistics demonstrates that cybercriminals began to launder four times more money in 2020. In 31% of cases, cybercriminals used malware to gain access to users' banking data 0. According to Kaspersky Lab, in 2020, theft of funds with the help of logins and passwords to accounts lost by users was in the second place: every third incident was associated with them (36%). Money-laundering incidents accounted for about 3% of attacks. For sophisticated money laundering schemes, scammers use automation tools, remote administration tools, proxies and the Tor browser to maintain anonymity. In particular, criminals use COVID-19 pandemic to realize financial fraudulent schemes, including the advertising and sale of counterfeit drugs, offering fraudulent investment opportunities and phishing schemes and spreading false information about COVID-19 exploiting virus-related fears. Thus, the number of fraudulent calls in Russia increased by 200%.

The most widespread among fraudsters is the legal program for delegating access TeamViewer, which allows an unauthorized person to connect to a smartphone. In this situation, the fraudster calls the victim and notifies that suspicious transactions have been recorded from the account. Then the fraudster asks to install the TeamViewer application on the smartphone and after gaining access to the victim's smartphone, the fraudster withdraws money from the bank account.

Today thefts are carried out by infecting the victim's computer or smartphone with malicious software. One of the most common methods of «infection» is phishing, which involves sending messages by SMS or e-mail identical to messages from a bank. Mailings are mainly carried out through «spoofing», which is a change in the sender's address, which is displayed to the recipient of the letter. The letter will contain a link, by clicking on which, the user will «infect» his phone.

It is considered that users of the operative Android and Windows are less secure than people using macOS and iOS devices. Since the share of macOS and iOS products on the world market is lower than that of Windows and Android, it is more profitable for hackers to develop malware with massive damage specifically for the latter.

One example is the dangerous Gustuff Trojan developed for Android-based mobile devices, which attacked clients of international banks, users of mobile crypto wallets and large e-commerce resources. Gustuff is distributed in a standard way via SMS messages containing links to download a malicious APK file. The Trojan also distinguished itself with one of its unique functions - in Group-IB it was called "auto-upload" into legitimate mobile banking applications and crypto-wallets. It is the realization of this possibility that allows Gustuff to accelerate and scale the theft of money. To auto-upload, the malware uses an Android operating system service known as the Accessibility Service 0.

It should be noted that many products that include AI technologies are developed by representatives of the private sector - FinTech companies. Thus, Feedzai offers OpenMLEngine data processing software that can detect and prevent money laundering and fraud. The Feedzai platform is usually integrated into the systems of a bank or service provider and only warns risk analysts about fraudulent cases that are deemed to be of high risk. Today, this software operates in the 10 largest US banks. Such a risk assessment system rejects new applications for accounts and only accepts clients with a low probability of committing fraud.

To monitor cyber threats and prevent cyberattacks, Darktrace has developed EnterpriseImmuneSystem software. One of the EnterpriseImmuneSystem software tools is DarktraceThreatVisualizer, which is a control panel that may be used by bank information security personnel to monitor cyber threats in real time. Today, more than 40 companies from various sectors of the economy are users of the software product.

In addition, the optimization of financial relations based on the introduction of IoT technologies will be carried out through the Enterprise Security System using the biometric data of customers. First of all, it will prevent criminals from guessing a

password or PIN-code, using a stolen card or copying it. Today only two countries, Colombia and Japan, have implemented a biometric data recognition system in ATMs 0.

To sum up, it is necessary to underline that banks have to focus on electronic platforms by introducing new technologies of outsourcing, the Internet of things and others. In the future, it is vital to create not only a workable system for ensuring cybersecurity in the credit and financial sector, including special supervisory units, but also to raise the culture of behavior in it of all participants in information exchange. Companies should be well aware that the advertising of various IoT systems is their responsibility for the quality of the services provided. Thus, companies need to have mechanisms to check the legality of transactions. Financial institutions should use secure software products for IoT systems, have qualified service personnel capable of responding to cyberattacks promptly and competently. Bank customers, in turn, need to improve their information literacy and comply with the rules for the safe use of a bank card.

In addition, many countries should improve their legislation due to the increasing number of crimes committed in cyberspace. It can also be concluded that to fully implement the laws on cybercrime, governments should provide resources to the legal enforcers and train them because one of the major impediments is the lack of resources needed to enforce the cybercrime law.

REFERENCES

1. Norman Mugarura, Emma Ssali – Intricacies of anti-money laundering and cyber-crimes regulation in a fluid global system. // Journal of Money Laundering Control. / Tekst elektronnyy. – 13 April, 2020.

2. Oluwatoyin Esther Akinbowale, Heinz Eckart Klingelhöfer and Mulatu Fekadu Zerihun – Analysis of cyber-crime effects on the banking sector using the balanced score card. // Journal of Financial Crime. / Tekst elektronnyy. – 16 June, 2020.

3. Revenkov P. V., Berdyugin A. A. – Cybersecurity in the internet of things and electronic banking. // National Interests: Priorities and Security. / Tekst elektronnyy. – August, 2016.

4. Official website of the Federal Service for Financial Monitoring. - Elektronnyy resurs. – URL: http://www.fedsfm.ru/activity/fatf (Date of address: 22.12.2020).

5. Poddubnyy I. V. - The use of remote access server and malware as means of theft from bank cards of citizens // Kriminalistika: vchera, segodnya, zavtra. - Tekst elektronnyy. – 2020.

6. The official website of the information agency Krasnaya Vesna. – Elektronnyy resurs. – URL: https://rossaprimavera.ru/news/184a9f29 (Date of address: 9.12.2020)